AMENDMENTS TO THE CLAIMS

1. (Previously Presented) A method for controlling access to an access protected unit, the method comprising:

reading at least one pair of absolute coordinates from an encoded base;

checking if the pair of coordinates are within a coordinate area belonging to an authorized user; and

granting access by the authorized user to the access protected unit if the coordinates are within the coordinate area belonging to the authorized user.

2. (Previously Presented) The method according to claim 1 wherein the reading at least one pair of coordinates further comprises:

recording a pattern from the base with a digital pen; and

converting the recorded pattern into a pair of coordinates.

3. (Original) The method according to claim 1 wherein the coordinate area is designated by two pairs of coordinates, the first coordinate pair designating one corner of the coordinate area and the second coordinate pair designating a second corner of the coordinate area, wherein the second coordinate pair lies diagonal to the first coordinate pair.

4. (Previously Presented) The method according to claim 1, wherein:

the reading reads a sequence of coordinate pairs corresponding to a displacement of a digital pen by the user, and the method further comprises:

MKM/JAV/kpc

checking if the sequence of coordinate pairs favorably compares to a stored sequence of

coordinate pairs belonging to the authorized user; and

granting access by the authorized user to the access protected unit if the sequence of

coordinate pairs favorably compares to the stored sequence of coordinate pairs belonging to the

authorized user.

5. (Original) The method of claim 4 wherein the stored sequence of coordinate pairs

corresponds to a signature of the authorized user.

6. (Previously Presented) The method according to claim 1, wherein

the reading reads a sequence of coordinate pairs corresponding to the displacement of a

digital pen by the user, and the method further comprises:

checking if the sequence of coordinate pairs favorably compares to a stored sequence of

coordinate pairs associated with the access protected unit; and

granting access by the authorized user to the access protected unit if the sequence of

coordinate pairs favorably compares to the stored sequence of coordinate pairs associated with

the access protected unit.

7. (Previously Presented) The method according to claim 1, wherein

the reading reads a sequence of coordinate pairs corresponding to a displacement of a

digital pen by the user, and the method further comprises:

MKM/JAV/kpc

checking if the sequence of coordinate pairs favorably compares to a stored sequence of

coordinate pairs associated with a program or function of the access protected unit; and

activating the program or function of the access protected unit if the sequence of

coordinate pairs favorably compares to the stored sequence of coordinate pairs associated with

the program or function of the access protected unit.

8. (Previously Presented) The method according to claim 1, further comprising:

reading an identification code from a digital pen;

checking if the identification code from the digital pen corresponds to an authorized

identification code; and

granting access by the authorized user to the access protected unit if the identification

code from the digital pen corresponds to the authorized identification code.

9. (Previously Presented) The method of claim 8, wherein checking if the identification

code from the digital pen corresponds to an authorized identification code, further comprises:

checking if the identification code from the digital pen corresponds to the at least one pair

of coordinates from the base.

10. (Previously Presented) The method of claim 8, wherein checking if the identification

code from the digital pen corresponds to an authorized identification code, further comprises

checking if the identification code from the digital pen corresponds to the authorized

identification code corresponding to the access protected unit.

4

MKM/JAV/kpc

11. (Currently Amended) A system for controlling a user's access to an access-protected

unit, comprising:

a user unit for reading at least one pair of absolute coordinates; and

a checking device which determines whether the at least one pair of coordinates are

associated with at least one coordinate area belonging to an authorized user for authorizing

access to the access-protected unit[[;]], and providing an enabling signal to the access protected

unit when the checking device determines that access is authorized.

12. (Original) The system of claim 11 wherein the user unit comprises an optical sensor

and image processor.

13. (Original) The system of claim 11 further comprising a base provided with a position

coding pattern, wherein said user unit is configured to read the position coding pattern from the

base and to convert the position coding pattern to the at least one pair of coordinates.

14. (Original) The system of claim 11, wherein the user unit is further operable to read a

sequence of coordinate pairs which describe displacement of the user unit when a user is writing

with the user unit.

15. (Original) The system of claim 14 wherein the checking device is operable to compare the sequence of coordinate pairs with a stored sequence of coordinate pairs and, on the basis of a favorable comparison, to provide an enabling signal to the access protected unit.

16. (Original) The system of claim 15 wherein the stored sequence of coordinate pairs represent a user's signature.

17. (Original) The system of claim 15 wherein the stored sequence of coordinate pairs represents a function or program within the access protected unit, and the checking device is operable to activate the function or program within the access protected unit based on the favorable comparison.

18. (Original) The system according to claim 11, wherein the checking device is integrated with the user unit.

19. (Original) The system according to claim 11, wherein the access protected unit is integrated with the user unit.

20. (Original) The system according to claim 11, wherein the access protected unit is a digital pen.

21. (Original) The system according to claim 11, wherein information about a plurality of coordinate areas is stored in the checking device.

MKM/JAV/kpc

22. (Original) The system according to claim 21, wherein the access protected unit is associated with at least one of said plurality of coordinate areas.

23. (Original) A system according to claim 21, wherein at least one authorized user identity is associated with at least one of said plurality of coordinate areas.

24. (Original) The system according to claim 11 further comprising a server unit in communication with the user unit and the access protected unit.

25. (Original) The system according to claim 24 wherein the user unit further comprises a wireless communication unit in communication with a network access unit in communication with the server unit.

26. (Original) The system according to claim 24 wherein the user unit further comprises a network access unit in communication with the server unit.

27. (Original) The system according to claim 24 wherein the user unit further comprises a wireless communication unit in communication with the server unit.

28. (Original) The system according to claim 24 wherein the checking device is integrated with the server unit.

29. (Previously Presented) The system according to claim 11 wherein the checking device is further operable to:

read an identification code from the user unit;

check if the identification code from the user unit corresponds to an authorized identification code; and

grant access by the user to the access protected unit if the identification code from the user unit corresponds to the authorized identification code.

30. (Previously Presented) A checking device for checking a user's access to an access protected unit, the checking device comprising:

memory for storing information about at least one coordinate area; and

a processor operative to:

receive at least one pair of absolute coordinates;

determine whether the at least one pair of coordinates are associated with the stored information for authorizing access to the access-protected unit;

provide an enabling signal to the access-protected unit if the processor determines that access is authorized.

31. (Previously Presented) The checking device according to claim 30 wherein the processor is further operative to check if the at least one pair of coordinates are lying within the at least one coordinate area for checking the user's authorization.

32. (Original) The checking device according to claim 30 wherein the memory is further operative to store a sequence of coordinate pairs and the processor is further operative to receive

a sequence of coordinate pairs and check the received sequence of coordinate pairs with the

stored sequence of coordinate pairs for checking the user's authorization.

33. (Original) The checking device according to claim 30, wherein the checking device is

integrated with the user unit.

34. (Original) The checking device according to claim 30 wherein the memory stores

information about a plurality of coordinate areas.

35. (Original) The checking device of claim 34 wherein the access protected unit is

associated with one of the plurality of coordinate areas.

36. (Original) The checking device of claim 34 wherein a program or function is

associated with one of the plurality of coordinate areas.

37. (Previously Presented) The checking device of claim 30 further comprising a

communications interface operably coupled to the processor.

38. (Previously Presented) The checking device of claim 37 wherein the communications

interface is operable to communicate with a server unit.

MKM/JAV/kpc

39. (Previously Presented) The checking device of claim 37 wherein the communications interface is operable to communicate with a user unit.

40. (Previously Presented) The checking device of claim 37 wherein the communications interface is a wireless interface.

41. (Previously Presented) The checking device of claim 37 wherein the communications interface is a hard-wired interface.

42. (Previously Presented) The checking device of claim 30 wherein the processor is further operable to:

read an identification code from a digital pen;

check if the identification code from the digital pen corresponds to an authorized identification code; and

grant access by the user to the access protected unit if the identification code from the digital pen corresponds to the authorized identification code.

43. (Previously Presented) A computer-readable medium containing instructions for controlling access to an access protected unit, the instructions comprising:

reading at least one pair of absolute coordinates from a base;

checking if the pair of coordinates are within a coordinate area belonging to an authorized user; and

MKM/JAV/kpc

granting access by the authorized user to the access protected unit if the coordinates are

within the coordinate area belonging to the authorized user.

44. (Original) The computer-readable medium of claim 43 wherein the instruction for

reading at least one pair of coordinates further comprise the instructions of:

recording a pattern from the base with a digital pen; and

converting the pattern into a pair of coordinates.

45. (Original) The computer-readable medium of claim 43 wherein the coordinate area is

designated by two pairs of coordinates, the first coordinate pair designating one corner of the

coordinate area and the second coordinate pair designating a second corner of the coordinate

area, wherein the second coordinate pair lies diagonal to the first coordinate pair.

46. (Previously Presented) The computer-readable medium of claim 43 wherein the

instructions further comprise the instructions of:

reading a sequence of coordinate pairs corresponding to a displacement of the digital pen

by the user;

checking if the sequence of coordinate pairs favorably compares to a stored sequence of

coordinate pairs belonging to the authorized user; and

granting access by the authorized user to the access protected unit if the sequence of

coordinate pairs favorably compares to the stored sequence of coordinate pairs belonging to the

authorized user.

47. (Original) The computer-readable medium of claim 46 wherein the stored sequence

of coordinate pairs corresponds to a signature of the authorized user.

48. (Previously Presented) The computer-readable medium of claim 43 wherein the

instructions further comprise the instructions of:

reading a sequence of coordinate pairs corresponding to a displacement of the digital pen

by the user;

checking if the sequence of coordinate pairs favorably compares to a stored sequence of

coordinate pairs associated with the access protected unit; and

granting access by the authorized user to the access protected unit if the sequence of

coordinate pairs favorably compares to the stored sequence of coordinate pairs associated with

the access protected unit.

49. (Original) The computer-readable medium of claim 43 wherein the instructions

further comprise the instructions of:

reading a sequence of coordinate pairs corresponding to the displacement of the digital

pen by the user;

checking if the sequence of coordinate pairs favorably compares to a stored sequence of

coordinate pairs associated with a program or function of the access protected unit; and

activating the program or function of the access protected unit if the sequence of

coordinate pairs favorably compares to the stored sequence of coordinate pairs associated with

the program or function of the access protected unit.

MKM/JAV/kpc

50. (Previously Presented) The computer-readable medium of claim 43 wherein the instructions further comprise the instructions of:

reading an identification code from the digital pen;

checking if the identification code from the digital pen corresponds to an authorized identification code; and

granting access by the authorized user to the access protected unit if the identification code from the digital pen corresponds to the authorized identification code.

51. (Original) The computer-readable medium of claim 50 wherein the instruction of checking if the identification code from the digital pen corresponds to an authorized identification code, further comprises the instruction of:

checking if the identification code from the digital pen corresponds to the at least one pair of coordinates from the base.

52. (Original) The computer-readable medium of claim 50 wherein the instruction of checking if the identification code from the digital pen corresponds to an authorized identification code, further comprises the instruction of:

checking if the identification code from the digital pen corresponds to the access protected unit.

MKM/JAV/kpc

53. (Previously Presented)   The method according to claim 4, wherein the stored sequence of coordinate pairs corresponds to one of a symbol and a sign.

54. (Previously Presented)   The method according to claim 1, wherein the reading further comprises:

optically reading the at least one pair of coordinates from the base, wherein the base is provided with a position coding pattern for coding a plurality of pairs of coordinates.

55. (Previously Presented) The system of claim 11, further comprising:

a plurality of user units for reading at least one pair of coordinates; and

a plurality of bases, each of which is provided with a subset belonging to a plurality of subsets of a position coding pattern, wherein each subset codes coordinates within a unique coordinate area.

56. (Previously Presented) The system of claim 15, wherein the stored sequence of coordinate pairs corresponds to one of a symbol and a sign.

57. (Previously Presented) The computer readable medium of claim 46, wherein the stored sequence of coordinate pairs corresponds to one of a symbol and a sign.

58. (Previously Presented) The system of claim 11, wherein the stored sequence of coordinate pairs corresponds to one of a symbol and a sign.

MKM/JAV/kpc

59. (Previously Presented) A base for controlling access to an access protected unit, comprising:

a substrate;

a writing field associated with the substrate; and

a position coding pattern associated with the writing field, wherein the position coding pattern encodes at least one pair of absolute coordinate positions used to grant access authorization.

60. (Previously Presented) The base according to claim 59, whereby the position coding pattern is read during an unformatted displacement of a user unit over the writing field, and wherein the user unit is configured to convert the position coding pattern to the at least one pair of coordinates.

61. (Previously Presented) The base according to claim 60, wherein the user unit is configured to read a sequence of coordinate pairs describing the displacement of the user unit, and further wherein the sequence of coordinate pairs are compared to a stored sequence of coordinate pairs for granting access authorization.

62. (Previously Presented) The base according to claim 61, wherein the stored sequence of coordinate pairs represents a user's signature.

MKM/JAV/kpc

63. (Previously Presented) The base according to claim 59, wherein the substrate is a card.

64. (Previously Presented) The base according to claim 63, wherein the card is substantially similar to a credit card with respect to size and material.

65. (Previously Presented) A method for controlling access to an access protected unit, comprising:

providing a position coding pattern associated with a writing field coupled to a base, wherein the position coding pattern encodes at least one pair of absolute coordinate positions used to grant access authorization;

moving a user unit in an unformatted manner in proximity to the writing field;

reading the position coding pattern during the moving;

converting the position coding pattern to the at least one pair of coordinates; and

granting access to an access protected unit based upon the at least one pair of coordinates.

66. (Previously Presented) The method according to claim 65, further comprising:

reading a sequence of coordinate pairs describing the displacement of the user unit; and

comparing the sequence of coordinate pairs are to a stored sequence of coordinate pairs for granting access authorization.

67. (Previously Presented) The method according to claim 66, wherein the stored sequence of coordinate pairs represents a user's signature.

68. (Previously Presented) The method according to claim 65, wherein the base is a card.

69. (Previously Presented) The method according to claim 1, wherein values of the at least one pair of absolute coordinates are not based upon a physical device which is separate from the base.

70. (Previously Presented) The method according to claim 69, wherein the physical device is a template.

MKM/JAV/kpc